

July 2020

CJEU INVALIDATES EU-US PRIVACY SHIELD FRAMEWORK AND INTRODUCES FURTHER RESTRICTIONS ON DATA TRANSFERS TO NON-EU COUNTRIES

On 16 July 2020, the Court of Justice of the European Union (CJEU) issued a long-awaited decision in a dispute between Facebook Ireland, the Irish Data Protection Authority and the Austrian data protection activist Maximilian Schrems.

Mr. Schrems filed a complaint in 2013 seeking to ban or restrict transfers of his personal data from the EU to third countries, specifically to the United States. Like many other internet service providers, Facebook had based data flows on the "EU-US Privacy Shield" Framework ("Privacy Shield") and EU model clauses for data transfers (Standard Contractual Clauses, "SCC"). The CJEU now invalidated "Privacy Shield" and clarified the requirements when employing SCC.

THE RULING

Based on the EU General Data Protection Regulation (GDPR) and fundamental rights under the Charter of Fundamental Rights of the European Union, the CJEU ruled as follows:

- The decision of the European Commission implementing "Privacy Shield" is invalid.
- SCC for the transfer of personal data to *processors* established in third countries remain valid.
- When transferring personal data to third countries based on SCC, the relevant aspects of the local legal system and especially any governmental access rights in these third countries must be examined *by all controllers and processors* on a case-by-case basis. Transmissions may only be conducted where a level of protection essentially equivalent to the fundamental rights guaranteed in the EU can *truly* be enforced.
- Supervisory authorities are required to act by suspending or prohibiting a transfer where the transfer is based on SCC that cannot be complied with.

CONSEQUENCES FOR INTERNATIONAL DATA TRANSFERS

While the invalidation of the Privacy Shield mechanism only affects data transfers to U.S. companies having self-certified under the Privacy Shield framework, other requirements, determined necessary by the CJEU for the assessment of local legal systems, create additional conditions for data transfers to any other third countries.






Data transfers to third countries, where the law of that third country allows its public authorities to interfere with the rights of the data subjects, must be stopped. Where such processing is not stopped by the data exporter, national supervisory authorities are required to suspend or prohibit a transfer, if it views the SCC are not or cannot be complied with.

If an adequacy decision of the Commission determines an adequate level of data protection in an individual third country, no further assessment is necessary. However, where data transfers are based on SCC, the adequacy of data protection obtained thereby must be scrutinized. Thus, the responsibility for assessing and ensuring adequate data protection for data transfers shifts entirely to companies.

If a supervisory authority assesses the level of data protection in the third country as inadequate, it will act and prohibit or suspend the transfer. The ECJ decision also highlights the possibility of data subjects to take action against illegal data transfers and to even claim damages in individual cases.

TAKE-AWAYS

The current map for data transfers to non-EU countries now reads as follows:

GDPR	Applicability	Description
Art 49		Necessary transfers remain unaffected (e.g. transfers relating to hotel bookings in third countries).
Art 45		Transfers based on an adequacy decision by the Commission remain unaffected (e.g. Switzerland, Japan, Channel Islands, Israel, New Zealand).
Art 45		Privacy Shield certifications no longer offer appropriate safeguards for data transfer to the U.S.A.
Art 46 (2) lit a, Art 47		Binding corporate rules remain a valid instrument for data transfers within a group. However, binding corporate rules require the approval of the competent supervisory authority.
Art 46 (2) lit c		When transferring data to a third country based on standard contractual clauses, the data exporter must review the enforceable rights and effective legal remedies for data subjects.

About WOLF THEISS

Wolf Theiss is one of the leading law firms in Central, Eastern and Southeastern Europe (CEE/SEE). We have built our reputation on a combination of unrivalled local knowledge and strong international capability. We opened our first office in Vienna over 60 years ago. Our team now brings together over 340 lawyers from a diverse range of backgrounds, working in offices in 13 countries throughout the CEE/SEE region.

For more information about our services, please contact:



Roland Marko
Partner
roland.marko@wolftheiss.com
T: +43 1 51510 5880



Paulina Pomorski
Senior Associate
paulina.pomorski@wolftheiss.com
T: +43 1 51510 5880



Johannes Sekanina
Associate
johannes.sekanina@wolftheiss.com
T: +43 1 51510 5880

This memorandum has been prepared solely for the purpose of general information and is not a substitute for legal advice.

Therefore, WOLF THEISS accepts no responsibility if – in reliance on the information contained in this memorandum – you act, or fail to act, in any particular way.

If you would like to know more about the topics covered in this memorandum or our services in general, please get in touch with your usual WOLF THEISS contact or with:

Wolf Theiss
Schubertring 6
AT – 1010 Vienna

www.wolftheiss.com